A Process for Developing and Balancing Quantitative Safety, Reliability, and Maintainability Requirements

Because of the interrelationships between system maintainability and reliability, it is important to consider their integrated effects on system-, element-, and component-level design, development, test, and evaluation. Tradeoffs must be evaluated in establishing system reliability and maintainability requirements because of their impact on nonrecurring and recurring costs and the minimization of system life cycle cost. System dependability and responsiveness attributes are both heavily influenced by achieving an effective balance between reliability and maintainability design characteristics. These attributes then drive the safety, cost, and operation of the system.

The process established for developing and balancing quantitative requirements for safety (S), reliability (R), and maintainability (M) derives and integrates Level I requirements and the controls needed to obtain program key objectives for safety and recurring cost (figure 1). Being quantitative, the process conveniently uses common mathematical models. Even though the process is shown as being worked from the top down, it can also be worked from the bottom up. Two illustrations using this process are provided.

This process uses three math models: (1) the binomial distribution (greater-than-or-equal-to case), (2) reliability for a series system, and (3) the Poisson distribution (less-than-or-equal-to case). The zero-fail case for the binomial distribution approximates the commonly known exponential distribution or "constant failure rate" distribution. Either model can be used. The binomial distribution was selected for modeling flexibility because it conveniently addresses both the zero-fail and failure cases. The failure case is typically used for unmanned spacecraft as with missiles.

As the first step of the process, the Systems Engineering designer begins with three inputs: (1) the desired number of missions the program is planning (n); (2) the minimum number of successful missions for duration of the program (x); and (3) the assurance (A) of obtaining x or more successes out of the n missions. In risk terms, 1–A is the probability or likelihood of not obtaining x or more successes out of n number of attempts or not obtaining the desired level of safety and reliability over the life of the system's program. When these three inputs are used in the binomial distribution, the minimum mission reliability (Ps) is calculated. At this point of the process, the Level I safety requirement has been established.

The second step uses the minimum mission reliability (Ps) and an estimate of the number of serial line replaceable unit (LRU) elements (e) as inputs into the formula for reliability of a series system to calculate minimum element reliability (Psi). Maximum element failure rate (Pfi) is equal to 1–Psi. Without considering the maintainability burden, which has a very large influence on recurring cost including the system's acquisition (fleet) size, the process at this point has established the safety and reliability requirements for the program. Table 1 (generated by the first two mentioned math models) provides values for Pfi at various levels of assurance (A) and quantities of serial systems (e) when x and n are both each equal to 100 missions.

The last step addresses the maintainability parameter, the parameter that provides a control for recurring costs resulting from maintenance and repair. Similar to assurance or program reliability (A), program maintainability (M) is a probability. The probability M is determined by the Poisson distribution and uses the following inputs: (1) the number of missions (n), (2) the number of elements (N, where $e \leq N$), (3) the LRU failure rate (Pfi or λ, where $\lambda \leq Pfi$), and (4)

the maximum number of LRU repairs (r). Technically, M is the probability of no more than r number of repairs occurring at a particular mission using e number of LRUs with an average failure rate of Pfi or λ. Table 2 (generated by the third mentioned math model) provides values for program maintainability (M) at various quantities of repairable system elements and repair rates.

To achieve the desired results in both M and the desired A, adjustments in e, Pfi, N, and λ must be made. These values become the enabling requirements to balance and achieve the desired key objectives of the program.

Illustration 1 (e = N case)

If A = 0.99 for 100 successes out of 100 attempts is required by program management and the current design concept calls for 100 serial systems (e = 100), then as per Table 1, Pfi ≈ 1×10^{-6} will satisfy the Assurance requirement. Additionally, if N = e = 100 and Pfi = λ = 1×10^{-6}, then as per Table 2, the probability of having no more than 1 repair per mission is 0.999999995. Thus, a Maintainability requirement desired at virtually any level for these management and system conditions is forecasted to be satisfied.

Illustration 2 (e < N case)

If A = 0.99 for 100 successes out of 100 attempts is required by program management, and the current design concept uses 100 serial systems (e = 100), then as per Table 1, Pfi ≈ 1×10^{-6} will satisfy the Assurance requirement. Additionally, if each of the 100 serial systems contains an average of 1,000 sub elements and each of the 100,000 sub elements (N = 1,000 × e = 1,000 × 100 = 100,000) has an average repair rate of λ = 1×10^{-5}, then as per Table 2, the probability of having no more than 1 repair per mission is 0.7356 or about 74 percent. In other words, this design concept under a 99-percent level of assurance indicates there is a 26-percent chance of having 2 or more (up to N) repairs for each of the 100 missions. Thus, if the Maintainability requirement was targeted to be no less than 90-percent, the Maintainability requirement is forecasted not to be satisfied--and the design parameters will need to be adjusted.

A Process for Developing and Balancing Quantitative Safety, Reliability, and Maintainability Requirements

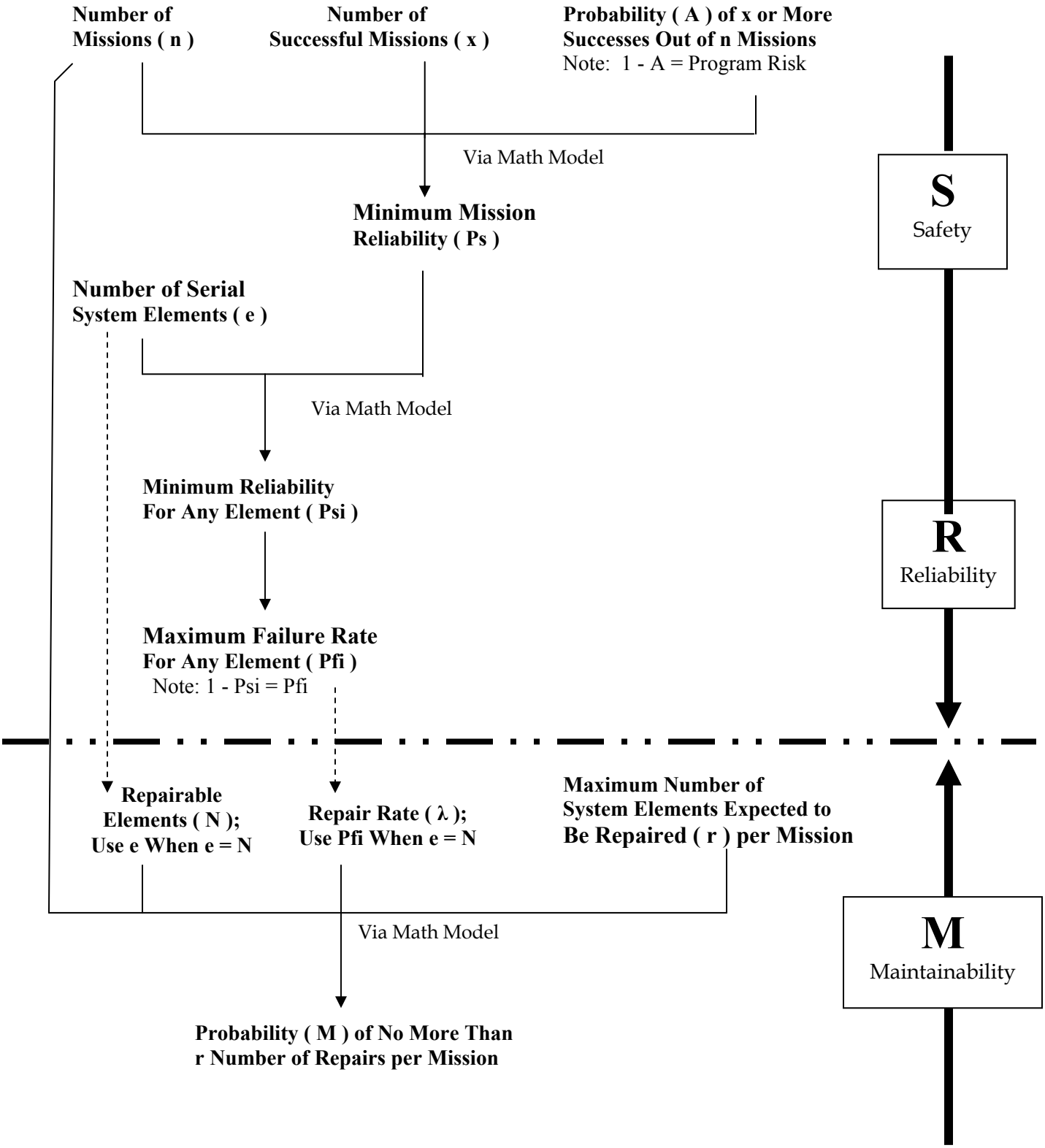

Figure 1

A Process for Developing and Balancing Quantitative Safety, Reliability, and Maintainability Requirements

Table 1. Safety (S) and Reliability (R): Maximum Failure Rate for Each Serial System (Pfi)

		Number of Serial Systems (e)				
		10^{+1}	10^{+2}	10^{+3}	10^{+4}	10^{+5}
Assurance (A)* (Probability of 100 Successes Out of 100 Attempts)	.90	1.0535×10^{-4}	1.0536×10^{-5}	1.0536×10^{-6}	1.0536×10^{-7}	1.0536×10^{-8}
	.95	5.1292×10^{-5}	5.1293×10^{-6}	5.1293×10^{-7}	5.1293×10^{-8}	5.1293×10^{-9}
	.99	1.0050×10^{-5}	1.0050×10^{-6}	1.0050×10^{-7}	1.0050×10^{-8}	1.0050×10^{-9}
	.999	1.0005×10^{-6}	1.0005×10^{-7}	1.0005×10^{-8}	1.0005×10^{-9}	1.0005×10^{-10}
*Assurance (A) is a composite of safety (S) and reliability (R).						

Table 2. Maintainability (M): Probability of No More Than One Element Repair per Mission

		Number of Subsystem Elements** (N) at the Repair or Maintenance Level				
		10^{+2}	10^{+3}	10^{+4}	10^{+5}	10^{+6}
Maximum Repair Rate for Each Element (λ)	10^{-3}	0.9953	0.7356	0.0005	0	0
	10^{-4}	0.99995	0.9953	0.7356	0.0005	0
	10^{-5}	0.9999995	0.99995	0.9953	0.7356	0.0005
	10^{-6}	0.999999995	0.9999995	0.99995	0.9953	0.7356
**When necessary, count legs in a redundant system as subsystem elements.						

Contacts: T.C. Adams (Timothy.C.Adams@nasa.gov), EA-C, (321) 867-2267 and R.E. Rhodes, YA-D4, (321) 867-6298

Key Words: Adams, T.C.; Rhodes, R.E.; system requirements, quantitative assurance requirements; safety, reliability, and maintainability requirements.